J1040 U.S. PTO
09/784151
02/16/01

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed h this Office.

出願年月日
Date of Application: ２０００年　６月３０日

願番号
Application Number: 特願２０００－１９９２６６

願人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年１０月２７日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０８８４９９

【書類名】　特許願

【整理番号】　0051232

【提出日】　平成12年 6月30日

【あて先】　特許庁長官　近藤　隆彦　殿

【国際特許分類】　G06F 11/36

【発明の名称】　ＬＳＩ，ＬＳＩを搭載した電子装置、デバッグ方法、ＬＳＩのデバッグ装置

【請求項の数】　13

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　川崎　雄介

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　橋本　繁

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100094514

【弁理士】

【氏名又は名称】　林　恒▲徳▼

【代理人】

【識別番号】　100094525

【弁理士】

【氏名又は名称】　土井　健二

【手数料の表示】

【予納台帳番号】　030708

出証特２０００－３０８８４９９

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9704944

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　ＬＳＩ，ＬＳＩを搭載した電子装置、デバッグ方法、ＬＳＩのデバッグ装置

【特許請求の範囲】

【請求項１】内部回路と、

外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、

前記デバッグＩ／Ｆ回路とデバッグ端子との間に設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と前記送信鍵とから認証を行い、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有することを

特徴とするＬＳＩ。

【請求項２】前記認証回路は、前記動作の許可のため、前記デバッグＩ／Ｆ回路へのリセット信号を解除することを

特徴とする請求項１のＬＳＩ。

【請求項３】前記認証回路は、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合することを

特徴とする請求項１のＬＳＩ。

【請求項４】前記認証回路は、前記動作許可の時間待ちを行うことを

特徴とする請求項１のＬＳＩ。

【請求項５】前記認証回路は、前記送信鍵を乱数により生成することを

特徴とする請求項１のＬＳＩ。

【請求項６】内部回路と、外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、前記デバッグＩ／Ｆ回路とデバッグ端子との間に設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有するＬＳＩを搭載したことを

特徴とする電子装置。

【請求項７】デバッグＩ／Ｆ回路を利用して、外部から内部回路をデバッグするデバッグ方法において、

出証特２０００－３０８８４９９

前記デバッグＩ／Ｆ回路の起動時に、前記外部に送信鍵を送信するステップと

、

前記外部から受信した信号と前記送信鍵とから認証を行い、前記デバッグＩ／Ｆ回路の動作を許可するステップとを有することを

特徴とするデバッグ方法。

【請求項８】前記認証ステップは、前記動作の許可のため、前記デバッグＩ／Ｆ回路へのリセット信号を解除するステップを有することを

特徴とする請求項７のデバッグ方法。

【請求項９】前記認証ステップは、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合するステップを有することを

特徴とする請求項７のデバッグ方法。

【請求項１０】前記認証ステップは、前記動作許可の時間待ちを行うステップを有することを

特徴とする請求項７のデバッグ方法。

【請求項１１】前記送信ステップは、前記送信鍵を乱数により生成するステップを有することを

特徴とする請求項７のデバッグ方法。

【請求項１２】デバッグ装置と前記デバッグＩ／Ｆ回路の間に設けられた識別装置が、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信するステップを、更に有することを

特徴とする請求項７のデバッグ方法。

【請求項１３】内部回路と、外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、前記デバッグＩ／Ｆ回路とデバッグ端子との間に設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有するＬＳＩをデバッグするデバッグ装置であって、デバッグユニットと前記デバッグＩ／Ｆ回路の間に設けられ、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信する識別装置を有することを

特徴とするデバッグ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＬＳＩの内部回路の挙動の不正取得を防止するためのセキュリテイ機能を有するＬＳＩ，電子装置、ＬＳＩのデバッグ方法、電子装置のデバッグ方法及びデバッグ装置に関する。

【０００２】

電子商取引等あらゆる分野で、よりセキュリティーの高い装置が求められている。このため、あらゆる方法で装置の逆解析（リバースエンジニアリング）を防ぐ方法が考案されてきた。しかし、これらの試みにもかかわらず、裏ＲＯＭ等が作成され、装置の開発者の不本意な用途に悪用される事が絶えない。このため、装置の動作そのものが、第三者に解析不能なシステムが求められている。

【０００３】

【従来の技術】

図９は、従来技術の説明図である。図９に示すように、ＬＳＩ１１０には、ＣＰＵ２００と周辺回路３００と、これらを接続するバス６００とが設けられている。このＬＳＩ１１０では、ＣＰＵ２００が、周辺回路３００からデータ、プログラムを取得し、データ処理して、データを周辺回路３００に出力する。

【０００４】

一方、このＬＳＩ１１０を使用して、装置を開発する場合には、ＣＰＵ２００の処理状況を、直接モニタし、プログラム等の検証を行う。周辺回路３００の出力データをモニタする検証方法も行われるが、出力に到るＣＰＵ２００の挙動は、出力データからは解明できない。

【０００５】

このため、ＣＰＵ２００に別のバス５００を介しデバッグＩ／Ｆ（インタフェイス）回路４００が設けられている。ＬＳＩ１１０外部のデバッグコントローラ１００は、このデバッグＩ／Ｆ４００に接続し、クロックＣＬＫを供給し、信号ＳＩＮを入力し、出力ＳＯＵＴを得る。

【０００６】

このデバッグＩ／Ｆ回路４００は、装置の開発時に、ＣＰＵ２００の挙動（プログラムカウンタ、レジスタ等の内容）を取得するのに、利用され、装置がフィールドに出荷された場合には、障害発生時、装置の診断時に、同様に利用される。

【０００７】

このような、デバッグＩ／Ｆ４００からのアクセスに対しては、従来は、セキュリテイ機能を設けていない。

【０００８】

【発明が解決しようとする課題】

従来の通常のセキュリティを要しない装置では、デバッグＩ／Ｆ端子は未使用時／使用時にかかわらず、外部から見えており第3者による利用に対して全く無防備である。このため、フィールドへ出荷された装置場合には、第3者がデバッグＩ／Ｆ端子を用いる事で，中央処理装置（CPU）の挙動を正確に逆解析する事が容易にでき、セキュリティー上無防備であるという問題がある。

【０００９】

従って、従来の装置では、デバッグＩ／Ｆ機能を設けたCPUを装置が用いている場合には、第三者に分析の手がかりを与える事になる。例えば、デバッグＩ／Ｆ機能付きのCPUを用いたPOSレジスタの場合には、デバッグＩ／Ｆのデバッグユニットとパソコン等を接続する事で，パスワードや暗号鍵等のデータですら容易に探し出す事が可能である。

【００１０】

従って、本発明の目的は、デバッグＩ／Ｆの利用を制限して、第３者の不正な逆解析を防止するためのＬＳＩ，電子装置、デバッグ方法及びデバッグ装置を提供するにある。

【００１１】

本発明の他の目的は、ＬＳＩ内のデバッグＩ／Ｆ回路と外部端子との間に認証ロジックを設け、デバッグＩ／Ｆの利用に制限を設けるためのＬＳＩ，電子装置、デバッグ方法及びデバッグ装置を提供するにある。

【００１２】

更に、本発明の他の目的は、ＬＳＩ内のデバッグＩ／Ｆ回路と外部端子との間に認証ロジックを解析することを防止するためのＬＳＩ，電子装置、デバッグ方法及びデバッグ装置を提供することにある。

【００１３】

更に、本発明の他の目的は、デバッグＩ／Ｆの利用を制限した第３者の不正な逆解析を、検出するためのＬＳＩ，電子装置、デバッグ方法、デバッグ方法及びデバッグ装置を提供するにある。

【００１４】

【課題を解決するための手段】

この目的の達成のため、本発明のＬＳＩは、内部回路と、外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、前記デバッグＩ／Ｆ回路とデバッグ端子との間に設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と前記送信鍵とから認証を行い、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有する。

【００１５】

本発明の電子装置は、内部回路と、外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、前記デバッグＩ／Ｆ回路とデバッグ端子との間に設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有するＬＳＩを搭載された。

【００１６】

本発明のデバッグ方法は、デバッグＩ／Ｆ回路の起動時に、前記外部に送信鍵を送信するステップと、前記外部から受信した信号と前記送信鍵とから認証を行い、前記デバッグＩ／Ｆ回路の動作を許可するステップとを有する。

【００１７】

本発明のデバッグ装置は、内部回路と、外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、前記デバッグＩ／Ｆ回路とデバッグ端子との間に

設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有するＬＳＩをデバッグするデバッグ装置であって、デバッグユニットと前記デバッグＩ／Ｆ回路の間に設けられ、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信する識別装置を有する。

【００１８】

デバッグＩ／Ｆ回路とデバッグ端子の間に認証回路を設けたため、第３者のデバッグＩ／Ｆを利用して、内部回路の動きをリバースエンジニアリングする等の不正行為から内部回路を守る事ができ，従来の装置よりもより高いセキュリティを保つ事ができる。

【００１９】

又、識別装置３とＬＳＩ２とのセットでセキュリテイを実現するため、物理的接続と認証アルゴリズムにより、セキュリテイを行うため、高いセキュリテイが可能となる。また、ＰＣ５による不正解析も困難である。

【００２０】

又、本発明のデバッグ方法では、前記認証ステップは、前記動作の許可のため、前記デバッグＩ／Ｆ回路へのリセット信号を解除するステップを有する。本発明のＬＳＩでは、前記認証回路は、前記動作の許可のため、前記デバッグＩ／Ｆ回路へのリセット信号を解除する。このため、認証しても、既存のリセットの解除により、実現できる。

【００２１】

更に、本発明のＬＳＩでは、前記認証回路は、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合する。本発明のデバッグ方法では、前記認証ステップは、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合するステップを有する。暗号化するため、より高いセキュリテイが可能となる。

【００２２】

本発明のＬＳＩでは、前記認証回路は、前記動作許可の時間待ちを行う。本発

明のデバッグ方法では、前記認証ステップは、前記動作許可の時間待ちを行うステップを有する。シリアルデータ鍵の判定前後に、タイマーを用いて、一致判定終了後の時間待ちをする。このため、第３者が、何らかの暗号鍵データを入力しても、認証結果（リセット）を得るまで時間がかかる。これにより、第３者による不正なデバッグＩ／Ｆ利用を防ぎ、また何度もリトライする際に莫大な時間がかかる。

【００２３】

本発明のＬＳＩでは、前記認証回路は、前記送信鍵を乱数により生成することにより、送信するシリアルデータ（送信鍵）を起動の毎に、乱数をベースにすることで、毎回異なる送受信データとして、解析を困難としている。

【００２４】

【発明の実施の形態】

以下、本発明を、ＬＳＩ，電子装置、他の実施の形態に分けて、説明する。

【００２５】

［ＬＳＩ］

図１は、本発明の一実施の形態のＬＳＩ及びデバッグ機構のブロック図であり、図２は、その認証処理の説明図、図３は、正当使用時の動作説明図、図４は、不正使用時の動作説明図である。

【００２６】

図１において、２はＣＰＵ付きシステムＬＳＩであり、本発明によるデバッグＩ／Ｆ利用認証回路が設けられている。１はＬＳＩ２内部のデバッグＩ／Ｆを利用するための外部デバッグコントローラである。３は識別装置であり、ＬＳＩ２とデバッグコントローラ１の間に挿入して用いられ、ＬＳＩ２内部の認証回路と連動し、認証を行う。

【００２７】

ＬＳＩ２は、デバッグＩ／Ｆ回路２－１と、ＣＰＵ２－２と、Ｉ／Ｆ回路２－１とＣＰＵ２－２を接続するデバッグバス４－１と、ＣＰＵバス４－２に接続された周辺回路２－１２とを有する。周辺回路２－１２は、ＬＳＩの用途により異なるが、例えば、図６以下で説明する電子マネー決済用回路である。

【００２８】

本発明の実施の形態では、このＣＰＵバス４－２に認証回路が設けられている。認証回路の構成を説明する。

【００２９】

ポート４－２は、バス４－２からＣＰＵ２－２の書き込みデータを受ける。レジスタ２－５は、ＣＰＵ２－２の生成したデバッグＩ／Ｆ利用送信鍵を格納する。レジスタ２－８は、ＣＰＵ２－２の生成した認証鍵を格納する。送信回路２－４は、識別装置３によって供給されているクロックに同期してレジスタ２－５の送信鍵を送信する。シフトレジスタ２－６は、識別装置２からの返送された暗号鍵を受信する。

【００３０】

一致検出回路２－９は、シフトレジスタ２－６の暗号鍵とレジスタ２－８の認証鍵と比較して、一致を検出する。タイマー回路２－７は、一致検出回路２－９の一致検出出力に応じて、クロックの計数を開始し、一定時間後、内部のデバッグＩ／Ｆ回路２－１へのリセット信号を解除する信号を生成する。リセットゲート２－１１は、リセット解除信号により、リセット信号のデバッグＩ／Ｆ回路２－１への入力を解除する。受信許可ゲート２－１０は、送信回路２－４からの受信許可信号に応じて、信号入力端子ＳＩＮからのデータを取り込むシフトレジスタ２－６をイネーブルにする。

【００３１】

次に、識別装置３には、鍵送受信回路３－１が設けられている。鍵送受信回路３－１は、識別装置３の電源が投入された時に、クロックを送信し、前述の送信鍵を受信して、あらかじめ決めておいたキーで暗号化して、暗号鍵を送信する。

【００３２】

次に、デバッグＩ／Ｆが利用可能となる動作手順を図１、図２により説明する。図１に示すように、デバッグＩ／Ｆを利用するデバッグコントローラ１を、識別装置３を介しＬＳＩ２に接続する。

【００３３】

①まず，ＬＳＩ２と識別装置３の電源を投入し起動する。すると、識別装置３

よりＬＳＩ２のデバッグＩ／Ｆ２－１へクロックが供給される。同時にＬＳＩ２内では，ＣＰＵ２－２が起動し，ファームウェアによりデバッグＩ／Ｆ利用送信鍵と認証鍵を生成し、バス４－２、ポート２－３を介しレジスタ２－５、２－８に書き込む。この時、送信鍵は乱数をベースに生成し、認証鍵は送信鍵をあらかじめ決めておいたキーを用いて暗号化して生成する。

【００３４】

②鍵が書き込まれると、識別装置３によって供給されているクロックに同期して、送信回路２－４が送信鍵を送信する。

【００３５】

③送信鍵を識別装置３内の鍵送受信回路３－１が受信して、あらかじめ決めておいたキーで暗号化して、暗号鍵を送信する。この時のキーは、先程ＬＳＩ２内のファームウェアによって用いたキーと同一のものである。

【００３６】

④ＬＳＩ２では、返送された暗号鍵をシフトレジスタ２－６にて受信し、一致検出回路２－９にて、レジスタ２－８の認証鍵と比較して、一致していた場合のみ、タイマー回路２－７へ一致検出を伝える。タイマー回路２－７では、一定時間待ってから、ゲート２－１１による内部のデバッグＩ／Ｆ２－１へのリセット信号を解除する。

【００３７】

こうして初めて、ＬＳＩ２のデバッグＩ／Ｆ回路２－１が利用可能となる。即ち、デバッグコントローラ１からリセット信号をＬＳＩ２に送信し、デバッグＩ／Ｆ回路２－１をリセットし、デバッグＩ／Ｆ回路２－１を利用して、ＣＰＵ２－２にアクセスできる。

【００３８】

図３に示すように、ＬＳＩ提供メーカーは、装置開発メーカーに、ＬＳＩ２と識別装置３とを提供する。ＬＳＩ２の暗号化キーと、識別装置３の暗号化キーとは、同一のものである。装置開発メーカーは、ＬＳＩ２をターゲットボード７に搭載し、装置の開発を行う。

【００３９】

デバッグを行う場合には、ＬＳＩ２に識別装置３を接続し、識別装置３にデバッグコントローラ１、ＰＣインタフェイスボード６、パーソナルコンピュータ５を接続する。識別装置３を間に入れると、前述の認証シーケンスが働き、リセットが解除されることで、ＰＣ５上のデバッガーが，デバッグＩ／Ｆ回路２－１を利用できるようになる。又、装置をフィールドに出荷した後も、識別装置３を接続することにより、ＰＣ５上のデバッガーが利用できるようになる。

【００４０】

一方、図４に示すように、識別装置３をつながない場合には、ＬＳＩ２のデバッグＩ／F回路２－１はリセットを解除されず、ＰＣ５のデバッガーは、ＬＳＩ２のＣＰＵ２－２をアクセス出来ない。例えば、装置のフィールドへの出荷後、第３者のデバッグＩ／Ｆを利用して、ＣＰＵ２－２内部の動きをリバースエンジニアリングする等の不正行為からＣＰＵ２－２を守る事ができ，従来の装置よりもより高いセキュリティを保つ事ができる。

【００４１】

即ち、従来のパスワードの認証等のセキュリテイ手法では、パスワードが漏れると、機能を発揮しなし、リトライにより、パスワードを解明しやすい。従って、多数のユーザーに提供されるＬＳＩ２のセキュリテイ機構として、不向きである。この実施の形態では、識別装置３とＬＳＩ２とのセットでセキュリテイを実現するため、物理的接続と認証アルゴリズムにより、セキュリテイを行うため、高いセキュリテイが可能となる。また、ＰＣ５による不正解析も困難である。

【００４２】

又、前述の利用認証機能は、暗号化アルゴリズムのため、巧妙な不正者は、認証機構の存在を知り、暗号化鍵（データ）のリトライにより解析を試みる場合がある。この実施の形態では、この解析を困難にするため、次の手法を採用している。

【００４３】

第１に、シリアルデータ鍵の判定後に、タイマー２－７を用いて、一致判定終了後の時間待ちをする。このため、第３者が、図４の接続で、何らかの暗号鍵データを入力しても、認証結果（リセット）を得るまで時間がかかる。これにより

、第３者による不正なデバッグＩ／Ｆ利用を防ぎ、また何度もリトライする際に莫大な時間がかかる。

【００４４】

第２に、送信するシリアルデータ（送信鍵）を起動の毎に、乱数をベースにすることで、毎回異なる送受信データとして、解析を困難としている。

【００４５】

第３に、シフトレジスタの受信動作を、送信鍵の送信後、一定時間とし、１回の起動時に、１回の受信しかしないようにし、繰り返しデータを入力しても受け付けないため、解析を困難としている。

【００４６】

次に、図５により、本発明の他の実施の形態の認証処理を説明する。

【００４７】

①まず，ＬＳＩ２と識別装置３の電源を投入し起動すると、識別装置３よりＬＳＩ２のデバッグＩ／Ｆ２－１へクロックが供給される。同時にＬＳＩ２内では，ＣＰＵ２－２が起動し，前述のように、ファームウェアによりデバッグＩ／Ｆ利用送信鍵と認証鍵を生成し、バス４－２、ポート２－３を介しレジスタ２－５、２－８に書き込む。

【００４８】

②鍵が書き込まれると、識別装置３によって供給されているクロックに同期して、送信回路２－４が送信鍵を送信する。

【００４９】

③送信鍵を識別装置３内の鍵送受信回路３－１が受信して、あらかじめ決めておいたキーで暗号化して、暗号鍵を送信する。この時のキーは、先程ＬＳＩ２内のファームウェアによって用いたキーと同一のものである。識別装置３では、暗号鍵にユーザーＩＤを付加し、ＬＳＩ２に送信する。

【００５０】

④ＬＳＩ２では、返送された暗号鍵をシフトレジスタ２－６にて受信し、一致検出回路２－９にて、レジスタ２－８の認証鍵と比較して、一致していた場合のみ、タイマー回路２－７へ一致検出を伝える。タイマー回路２－７では、一定時

間待ってから、ゲート２－１１の内部のデバッグＩ／Ｆ２－１へのリセット信号の入力を解除する。又、ユーザーＩＤは、ログされる。このため、万一、送信鍵の情報が漏れた際に、ログされたユーザーＩＤから、どのユーザーから漏れたかを特定できる。

【００５１】

この実施の形態において、識別装置３で、受信した送信鍵とユーザーＩＤとをキーで暗号化する方法を採用することにより、ユーザーＩＤが容易に変更されることを防止できる。

[電子装置]

次に、前述のシステムＬＳＩ２を搭載した電子装置を説明する。図６は、システムＬＳＩ２の適用例の説明図であり、図７は、この適用例でのＬＳＩ２の周辺回路の構成図、図８は、電子装置の説明図である。

【００５２】

図６に示すものでは、システムＬＳＩ２は、カード決済用ＬＳＩであり、デビットカード決済機能４０、クレジットカード決済機能４１、電子マネー決済機能４２、その他のサービス機能４３を有する。このため、ＬＳＩ２には、ＩＣカードリーダ／ライタ３０と、磁気カードリーダ３１と、表示及びキー３２とが接続される。又、必要に応じて、レシートプリンタ３３が接続される。これらの決済機能４０～４３は、ＬＳＩ２のＣＰＵ２－２のプログラムの実行により、実現される。

【００５３】

従って、このＬＳＩ２を搭載することにより、各種の電子装置５０～５７に、カード決済機能を付与できる。これらの電子装置は、例えば、ＰＯＳ用リーダ／ライタ５０、統合端末５１、モバイル端末５２、ＡＴＭ（自動テラーマシン）５３、自動販売機５４、ＰＤＡ（パーソナル機器）５５、携帯電話５６、ＰＣ（パーソナルコンピュータ）５７である。

【００５４】

このカード決済のためのＬＳＩ２の周辺回路２－１２を、図７により、説明する。周辺回路２－１２は、スマートカードコントローラ６０と、ＭＳ制御回路６

１と、ＬＣＤ制御回路６２と、マトリクスＫＢ制御回路６３と、メモリコントローラ６４と、シリアル入出力ポート６９～７２とを有する。図７では、前述のＬＳＩ２は、ターゲットボード７に搭載された状態を示し、ＬＳＩ２を説明の簡単のため、ＣＰＵ２－２と周辺回路２－１２（６０－６４、６９－７２）のみ示してある。勿論、デバッグＩ／Ｆ２－１，認証回路を有する。

【００５５】

スマートカードコントローラ６０は、ＩＣカードリーダ／ライタ３０を介しＩＣカード（スマートカードという）のデータのリード／ライトを行う。ＭＳ制御回路６１は、ＭＳ（磁気ストライプ）リーダ３１の制御を行う。ＬＣＤ制御回路６２は、ＬＣＤ（液晶デイスプレイ）３２－１の表示制御を行う。マトリクスＫＢ制御回路６３は、テンキー３２－２の入力を認識する。メモリコントローラ６４は、ボード７上の各種メモリ（ＲＯＭ６５、ＳＲＡＭ６６、ＦＬＡＳＨ６７、ＳＤＲＡＭ６８）との入出力制御を行う。シリアルポート６９～７２は、シリアルデータの入出力を行うため、ボード７のドライバ７３～７５に接続される。これらは、いずれもＣＰＵバス４－２に接続される。

【００５６】

図８は、決済用ＬＳＩが搭載された電子装置のシステム構成図であり、ＰＯＳシステムを示している。ネットワーク３５に、ストアコントローラ２０と、複数のＰＯＳ１０が接続されている。ＰＯＳ１０には、ＩＣカードリーダ／ライタ３０が接続されている。ストアコントローラ２０と、複数のＰＯＳ１０とには、前述の決済用ＬＳＩ（ＩＦＤという）２が設けられ、決済データを直接やりとりする。

【００５７】

顧客のＩＣカード３４－１は、ＩＦＤ２を介しＰＯＳ用ＩＣカード３４－２と交信し、ＰＯＳ用ＩＣカード３４－２は、ＩＦＤ２，ターミナルコントローラ１１、ネットワーク３５、ターミナルコントローラ１１、ＩＦＤ２を介しストアコントローラ２０のＩＣカード３４－２と交信する。

【００５８】

例えば、ＩＣカードで電子決済を行う場合には、顧客のＩＣカード３４－１の

データは、ＩＦＤ２を介しＰＯＳ用ＩＣカード３４－２に格納される。その後、ＰＯＳ用ＩＣカード３４－２の格納データは、ＩＦＤ２，ターミナルコントローラ１１、ネットワーク３５、ターミナルコントローラ１１、ＩＦＤ２を介しストアコントローラ２０のＩＣカード３４－２に格納される。

【００５９】

このシステムでは、ＩＦＤ２により、電子決済データのルートがクローズしているため、決済データ（パスワード、口座番号、残高等）が漏れるおそれがないため、安全性が高い。

【００６０】

しかし、前述のように、デバッグＩ／Ｆを利用して、ＣＰＵ２－２にアクセスすれば、決済データ（パスワード、口座番号、残高等）を不正取得でき、悪用されるおそれがある。従って、本発明の認証機構は、このような用途に特に有効である。

【００６１】

［他の実施の形態］

上述の実施の態様の他に、本発明は、次のような変形が可能である。

（１）前述の実施の形態では、認証により、リセット信号を解除しているが、デバッグＩ／Ｆ２－１のクロック入力側に、ゲートを設け、認証により、クロック入力を許可するようにしても良い。

（２）前述の実施の形態では、一致判定後、タイマーで時間待ちしたが、一致判定前に、タイマーで判定の時間待ちをおこなうこともできる。

（３）一致判定により、不一致を検出した場合には、これを周辺回路に通知すると良い。これにより、周辺回路は、不正アクセスと判定し、例えば、セキュリテイの必要なデータを消去する等の処置をとることができる。

（４）システムＬＳＩをカード決済用で説明したが、他の用途のものに用いても良い。

（５）ＣＰＵのデバッグＩ／Ｆで説明したが、他の回路のデバッグＩ／Ｆに適用できる。

【００６２】

以上、本発明を実施の形態により説明したが、本発明の主旨の範囲内で種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【００６３】

（付記）

（付記１）内部回路と、外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、前記デバッグＩ／Ｆ回路とデバッグ端子との間に設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と前記送信鍵とから認証を行い、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有することを特徴とするＬＳＩ。

【００６４】

（付記２）前記認証回路は、前記動作の許可のため、前記デバッグＩ／Ｆ回路へのリセット信号を解除することを特徴とする付記１のＬＳＩ。

【００６５】

（付記３）前記認証回路は、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合することを特徴とする付記１のＬＳＩ。

【００６６】

（付記４）前記認証回路は、前記動作許可の時間待ちを行うことを特徴とする付記１のＬＳＩ。

【００６７】

（付記５）前記認証回路は、前記送信鍵を乱数により生成することを特徴とする付記１のＬＳＩ。

【００６８】

（付記６）内部回路と、外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、前記デバッグＩ／Ｆ回路とデバッグ端子との間に設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有するＬＳＩを搭載したことを特徴とする電子装置。

【００６９】

（付記７）前記認証回路は、前記動作の許可のため、前記デバッグＩ／Ｆ回路へのリセット信号を解除することを特徴とする付記６の電子装置。

【００７０】

（付記８）前記認証回路は、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合することを特徴とする付記６の電子装置。

【００７１】

（付記９）前記認証回路は、前記動作許可の時間待ちを行うことを特徴とする付記６の電子装置。

【００７２】

（付記１０）前記認証回路は、前記送信鍵を乱数により生成することを特徴とする付記６の電子装置。

【００７３】

（付記１１）デバッグＩ／Ｆ回路を利用して、外部から内部回路をデバッグするデバッグ方法において、前記デバッグＩ／Ｆ回路の起動時に、前記外部に送信鍵を送信するステップと、前記外部から受信した信号と前記送信鍵とから認証を行い、前記デバッグＩ／Ｆ回路の動作を許可するステップとを有することを特徴とするデバッグ方法。

【００７４】

（付記１２）前記認証ステップは、前記動作の許可のため、前記デバッグＩ／Ｆ回路へのリセット信号を解除するステップを有することを特徴とする付記１１のデバッグ方法。

【００７５】

（付記１３）前記認証ステップは、前記送信鍵を所定のキーで暗号化した認証鍵を生成し、前記受信信号と前記認証鍵とを照合するステップを有することを特徴とする付記１１のデバッグ方法。

【００７６】

（付記１４）前記認証ステップは、前記動作許可の時間待ちを行うステップを有することを特徴とする付記１１のデバッグ方法。

【００７７】

（付記１５）前記送信ステップは、前記送信鍵を乱数により生成するステップを有することを特徴とする付記１１のデバッグ方法。

【００７８】

（付記１６）デバッグ装置と前記デバッグＩ／Ｆ回路の間に設けられた識別装置が、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信するステップを、更に有することを特徴とする付記１１のデバッグ方法。

【００７９】

（付記１７）内部回路と、外部から前記内部回路をデバッグするためのデバッグＩ／Ｆ回路と、前記デバッグＩ／Ｆ回路とデバッグ端子との間に設けられ、前記デバッグＩ／Ｆ回路の起動時に、前記デバッグ端子から外部に送信鍵を送信し、前記デバッグ端子から受信した信号と照合し、前記デバッグＩ／Ｆ回路の動作を許可する認証回路とを有するＬＳＩをデバッグするデバッグ装置であって、デバッグユニットと前記デバッグＩ／Ｆ回路の間に設けられ、前記送信鍵を受信し、所定のキーで暗号化して、前記受信信号を送信する識別装置を有することを特徴とするデバッグ装置。

【００８０】

【発明の効果】

以上説明したように、本発明によれば、次の効果を奏する。

【００８１】

デバッグＩ／Ｆ回路とデバッグ端子の間に認証回路を設けたため、第３者のデバッグＩ／Ｆを利用して、内部回路の動きをリバースエンジニアリングする等の不正行為から内部回路を守る事ができ，従来の装置よりもより高いセキュリティを保つ事ができる。

【００８２】

又、識別装置３とＬＳＩ２とのセットでセキュリテイを実現するため、物理的接続と認証アルゴリズムにより、セキュリテイを行うため、高いセキュリテイが可能となる。また、ＰＣ５による不正解析も困難である。

【図面の簡単な説明】

【図１】

本発明の一実施の形態のＬＳＩのブロック図である。

【図２】

図１の認証処理の説明図である。

【図３】

図１のＬＳＩのデバッグ方法の説明図である。

【図４】

図１のＬＳＩの不正アクセス防止の説明図である。

【図５】

図１の他の認証処理の説明図である。

【図６】

図１のＬＳＩを搭載した電子装置の説明図である。

【図７】

図１の周辺回路のブロック図である。

【図８】

図６のＬＳＩを搭載したＰＯＳシステムの構成図である。

【図９】

従来技術の説明図である。

【符号の説明】

１　デバッグコントローラ

２　ＬＳＩ

３　識別装置

２－１　デバッグＩ／Ｆ回路

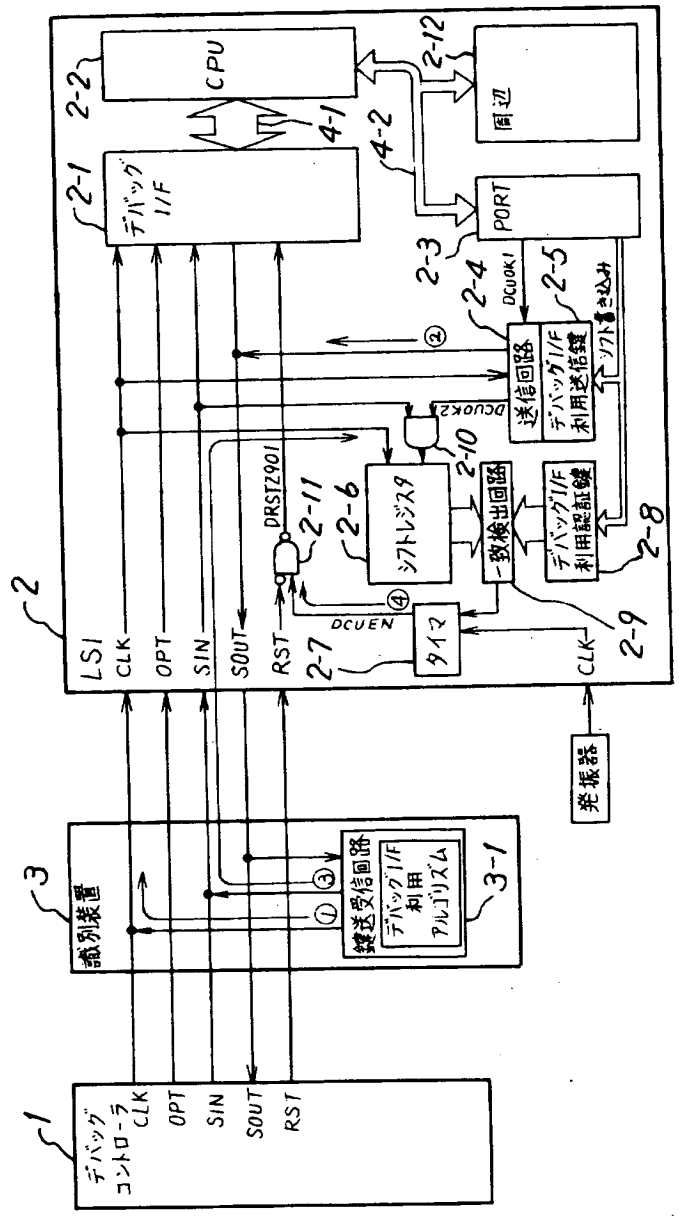
２－２　ＣＰＵ

２－３～２－１１　認証回路

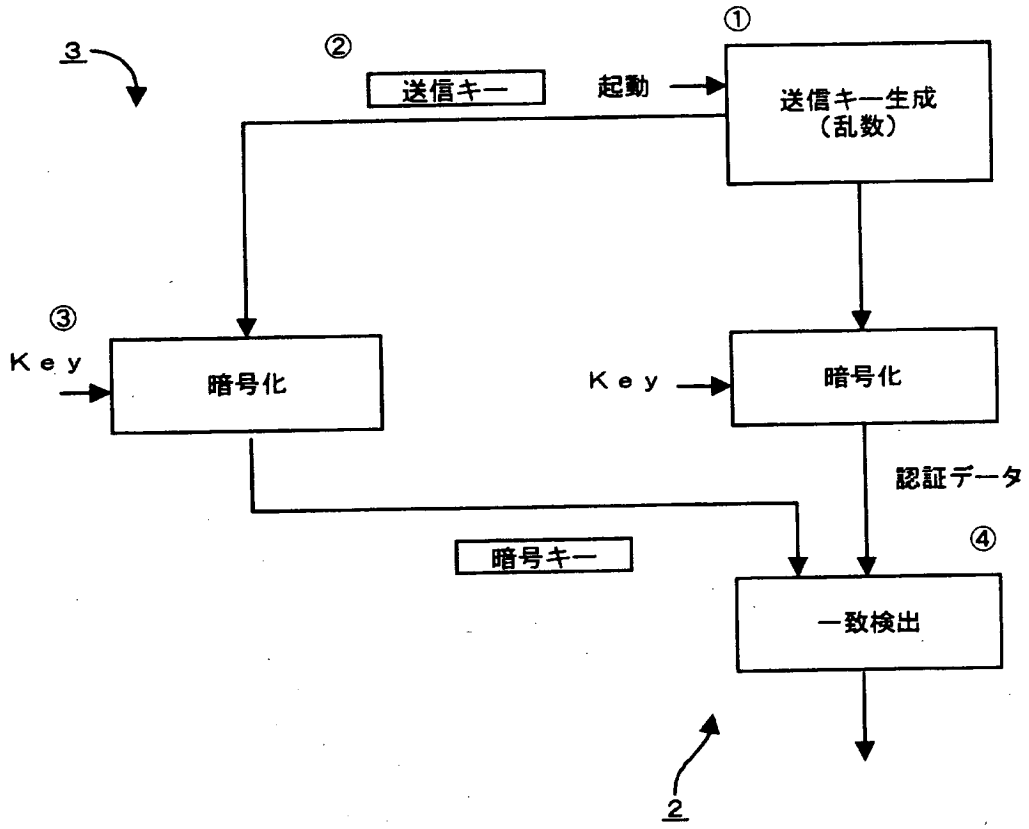
２－１２　周辺回路

【書類名】　　図面

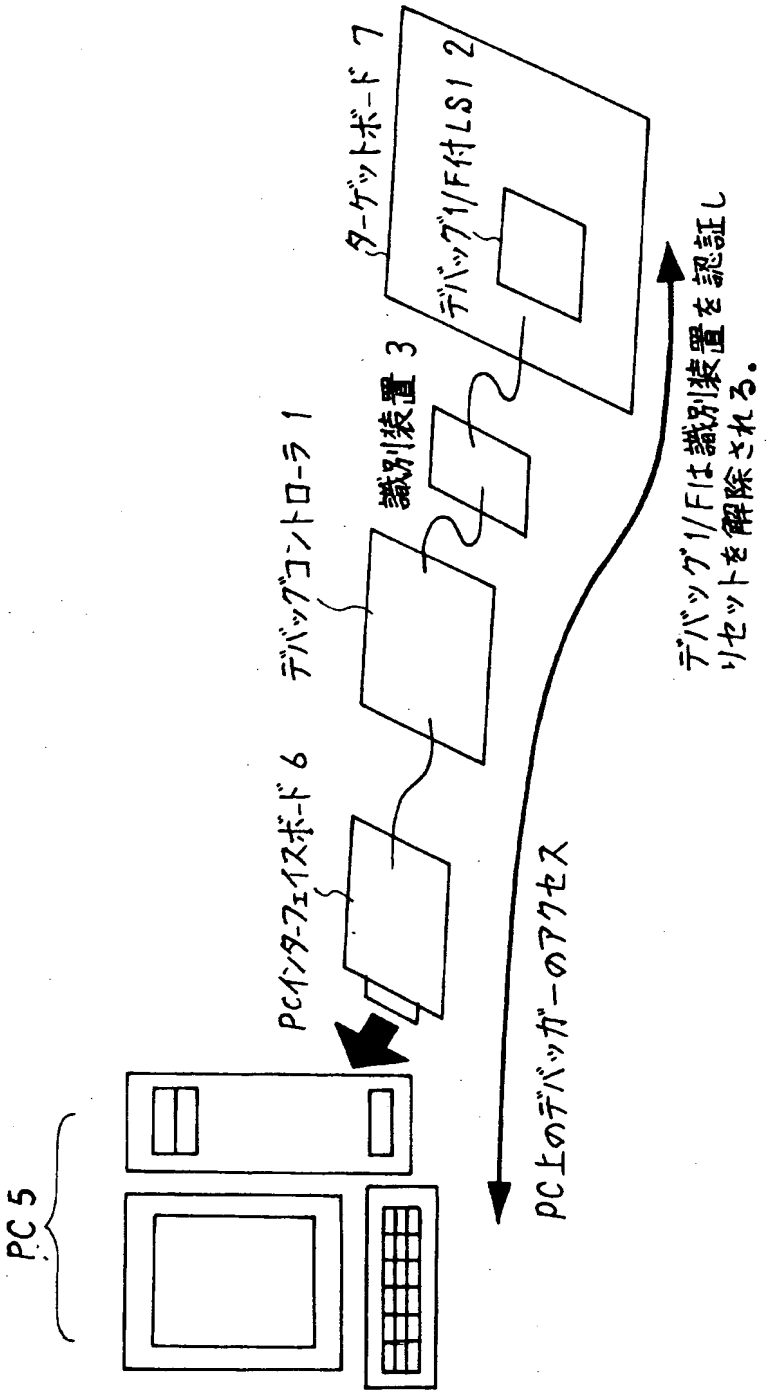
【図１】


CPU
2-2
デバッグ I/F
2-1
4-1
4-2
周辺
2-12
PORT
2-3
2-4
DCUOK1
2-5
送信回路
デバッグI/F 利用送信鍵
ソフトで書き込み
DCUOK2
2-10
シフトレジスタ
2-6
一致検出回路
デバッグI/F 利用認証鍵
2-8
DRSTZ901
2-11
DCUEN
タイマ
2-7
LSI
CLK
OPT
SIN
SOUT
RST
2-9
発振器
識別装置
3
鍵送受信回路
デバッグI/F 利用 アルゴリズム
3-1
デバッグ コントローラ
1

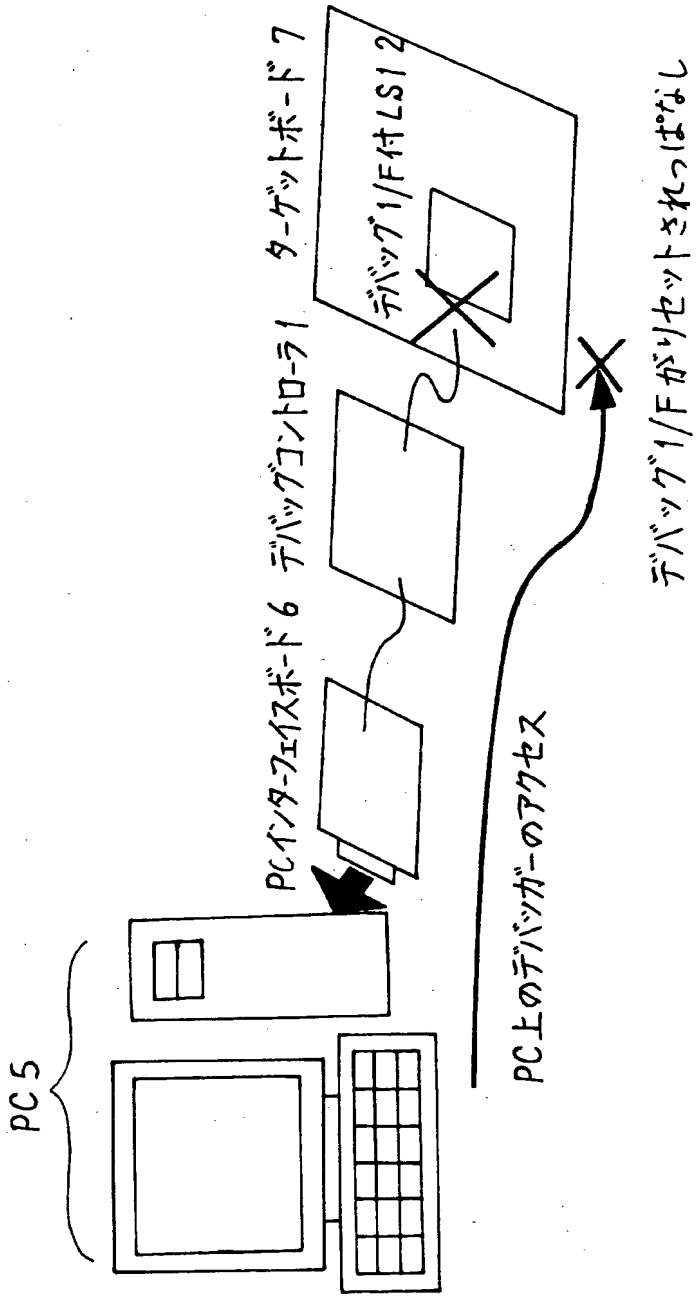
【図２】



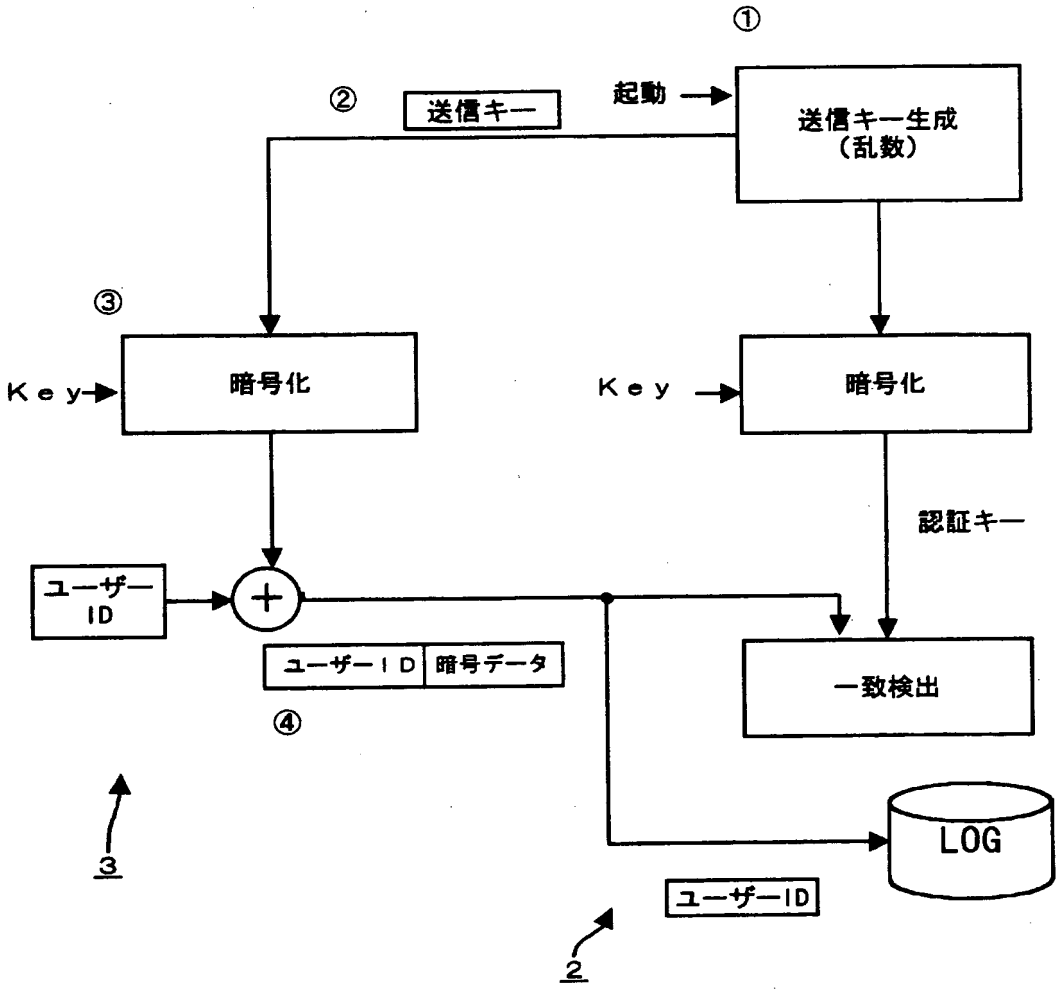
【図３】


PC 5
PCインターフェイスボード 6
デバッグコントローラ 1
識別装置 3
ターゲットボード 7
デバッグI/F付LSI 2
PC上のデバッガーのアクセス
デバッグI/Fは識別装置を認証し
リセットを解除される。

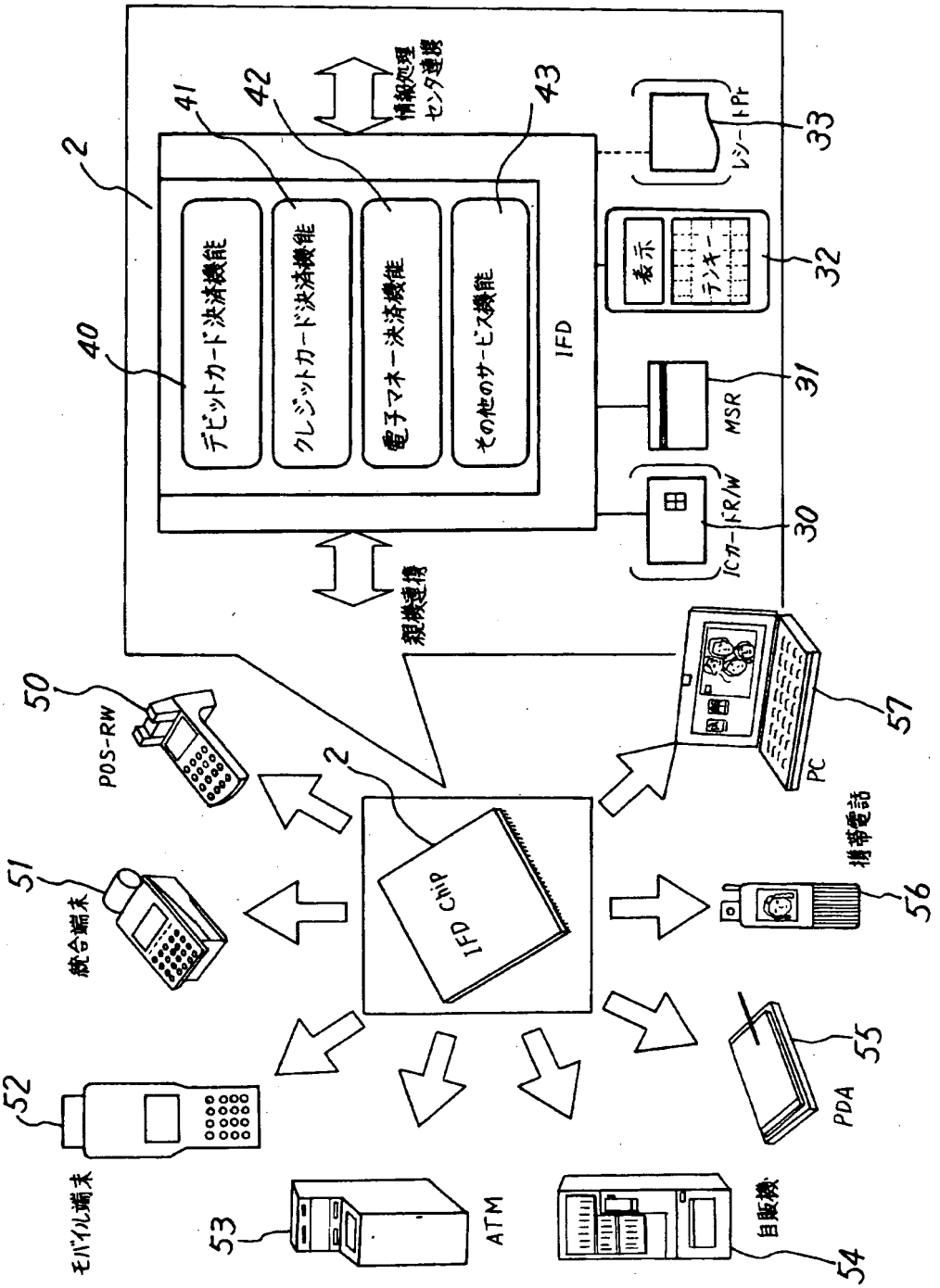
【図４】


PC5
PCインターフェイスボード6
デバッグコントローラ1
ターゲットボード7
デバッグI/F付LSI2
デバッグI/Fがリセットされっぱなし
PC上のデバッガーのアクセス

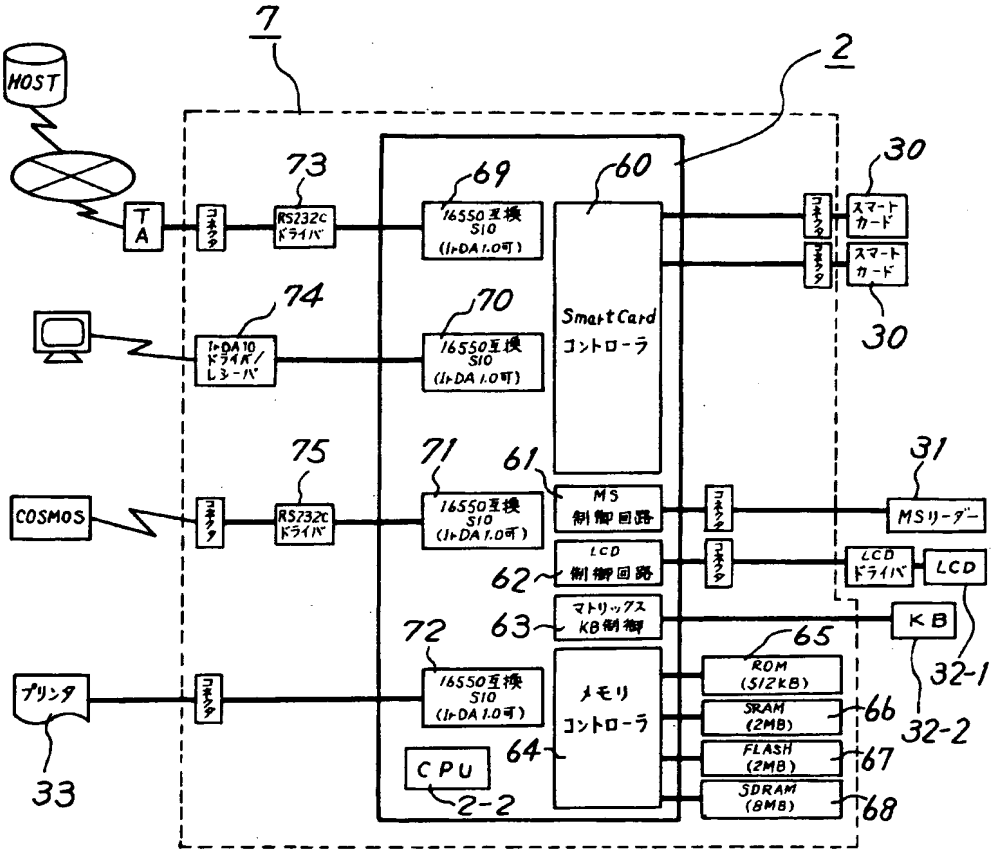
【図５】


①
②
送信キー
起動
送信キー生成
（乱数）
③
Ｋｅｙ
暗号化
Ｋｅｙ
暗号化
認証キー
ユーザー
ID
ユーザーＩＤ
暗号データ
④
一致検出
LOG
3
ユーザーID
2

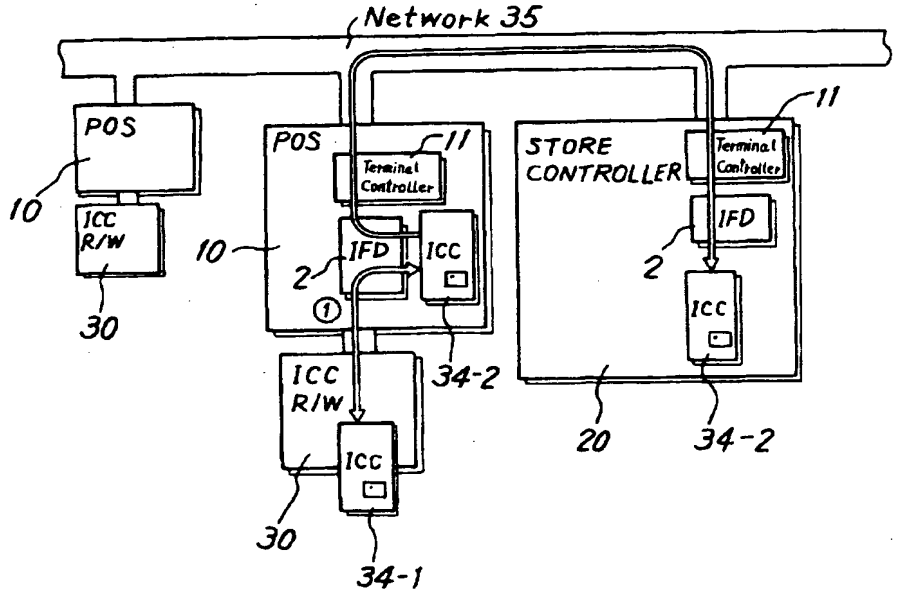
【図６】


2
41
42
43
情報処理センタ連携
レシートPr
33
表示
テンキー
32
40
デビットカード決済機能
クレジットカード決済機能
電子マネー決済機能
その他のサービス機能
IFD
MSR
31
ICカードR/W
30
親機連携
50
POS-RW
2
IFD Chip
PC
57
51
統合端末
携帯電話
56
52
モバイル端末
53
ATM
PDA
55
自販機
54

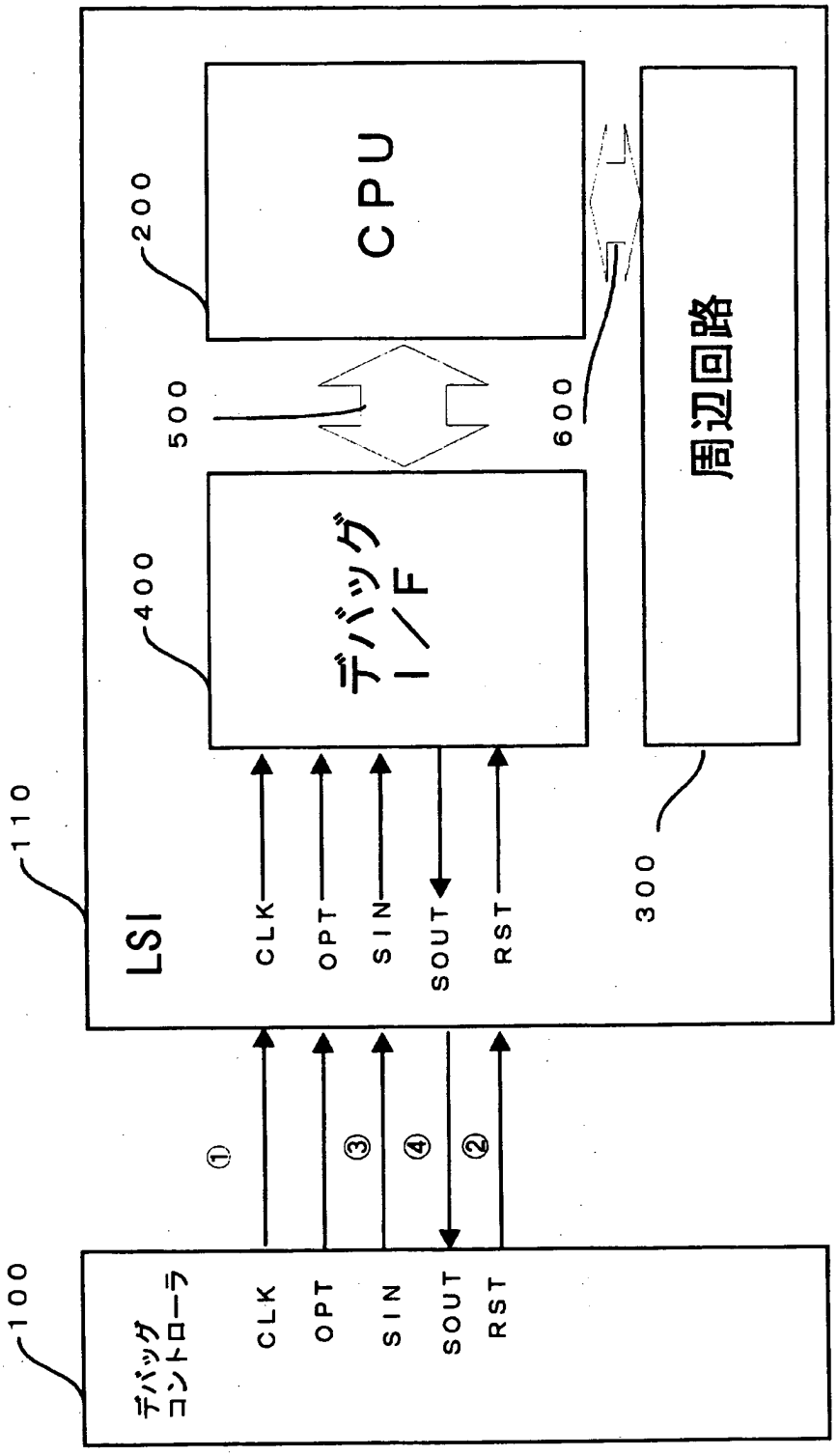
【図７】


7
2
HOST
TA
コネクタ
RS232C ドライバ
73
69
16550互換 SIO (IrDA1.0可)
60
30
スマートカード
74
IrDA1.0 ドライバ/レシーバ
70
SmartCard コントローラ
COSMOS
75
71
61
MS 制御回路
31
MSリーダー
LCD 制御回路
62
LCD ドライバ
LCD
マトリックス KB制御
63
KB
32-1
32-2
72
65
ROM (512kB)
SRAM (2MB)
66
FLASH (2MB)
67
SDRAM (8MB)
68
メモリ コントローラ
64
CPU
2-2
プリンタ
33

【図８】


Network 35
POS
10
ICC R/W
30
POS
11
Terminal Controller
10
IFD
ICC
2
①
34-2
ICC R/W
ICC
30
34-1
STORE CONTROLLER
11
Terminal Controller
IFD
2
ICC
20
34-2

【図９】


CPU
200
500
600
周辺回路
デバッグ
I／F
400
LSI
110
300
CLK
OPT
SIN
SOUT
RST
①
③
④
②
デバッグ
コントローラ
100
CLK
OPT
SIN
SOUT
RST

【書類名】　要約書

【要約】

【課題】　システムＬＳＩにおいて、デバッグＩ／Ｆからの内部回路へのアクセスを制限する。

【解決手段】　デバッグＩ／Ｆ回路（２－１）とデバッグ端子の間に、認証回路（２－３～２－１１）を設ける。認証回路は、起動時に、外部に送信鍵を送信し、受信信号と送信鍵から認証を行い、デバッグＩ／Ｆへのアクセスを許可する。認証回路により、デバッグＩ／Ｆからの第３者の不正アクセスを防止できる。

【選択図】　図１

出証特２０００－３０８８４９９

認定・付加情報

特許出願の番号	特願２０００－１９９２６６
受付番号	５００００８２４３８５
書類名	特許願
担当官	高田　良彦　　２３１９
作成日	平成１２年　７月　７日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】	富士通株式会社

【代理人】　申請人

【識別番号】	100094514
【住所又は居所】	神奈川県横浜市港北区新横浜３－９－５　第三東昇ビル３階　林・土井　国際特許事務所
【氏名又は名称】	林　恒徳

【代理人】

【識別番号】	100094525
【住所又は居所】	神奈川県横浜市港北区新横浜３－９－５　第三東昇ビル３階　林・土井　国際特許事務所
【氏名又は名称】	土井　健二

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社